



Investigation by CipherTrace of My Big Coin

18 May 2022

At the behest of the United States Department of Justice, CipherTrace investigated My Big Coin. CipherTrace provided an initial report dated April 9, 2020. This document supplements that report.

Pamela Clegg, of CipherTrace, produced this supplemental report to offer an official expert opinion report and document the investigation in support of that opinion. The initial report was a snapshot of information and findings to assist in making a decision about the case.

Part I: Witness Qualifications

Pamela A. Clegg is a leading expert on cryptocurrency investigations. Ms. Clegg has more than 15 years of diplomatic and private sector experience working on cutting-edge national security issues, including money laundering and fraud investigations relating to counterterrorism, counternarcotics, security, and nation building. This service expanded over many diverse and challenging locations worldwide. Ms. Clegg obtained her Certified Anti-Money Laundering Specialist (CAMS) in March 2018.

Ms. Clegg created and authored multiple cryptocurrency training courses and taught thousands of students around the world in the area of cryptocurrency investigations and compliance. Ms. Clegg has conducted trainings and given presentations internationally on cryptocurrency and financial crimes, including to Interpol, Europol, Department of Treasury, Department of Homeland Security and Department of Justice. She created and implemented certification courses that are attended by public and private sector investigators, compliance officers, and managers, and include:

1. Blockchain & Cryptocurrency Essentials Certification (BCEC). BCEC is a foundational course for executives new to cryptocurrency and blockchain. Participants learn the essentials behind blockchain and distributed ledger technology (DLT), how cryptocurrency transactions work, VASP typologies, industry trends, and the role blockchain analytics plays in the crypto ecosystem
2. Cryptocurrency Tracing Certified Examiner (CTCE). CTCE provides hands-on instruction in blockchain and cryptocurrency tracing. Participants develop and hone digital investigation techniques as they learn a risk-based approach to tracing the source of blockchain funds and de-anonymizing cryptocurrency transactions with cryptocurrency forensic tools.
3. Certified Cryptocurrency Risk Specialist (CCRS). CCRS provides the necessary knowledge base for financial institutions to have the ability to comply with regulatory requirements for identifying, assessing, and mitigating cryptocurrency risk exposure. CCRS also examines the best practices for pre-onboarding of corporate clients in the virtual currency space and to optimize existing compliance policies where necessary in accordance with evolving regulatory requirements, including specific country requirements as they relate to virtual asset businesses. It also delves into compliance issues and requirements pertinent to custodial solutions.

Ms. Clegg has authored multiple writings, including:

- 1) June 2021: Ransomware Seizure: Blockchain Analysis Helps US Authorities Seize Over \$2 Million in DarkSide Ransom Paid by Colonial Pipeline
<https://ciphertrace.com/ransomware-seizure-blockchain-analytics-helps-us-authorities-seize-over-2-million-in-darkside-ransom-paid-by-colonial-pipeline/>
- 2) April 2021: Blockchain Analytics—the Secret Weapon to Combatting Ransomware

<https://ciphertrace.com/blockchain-analytics-the-secret-weapon-to-combatting-ransomware/>

- 3) December 2020: Only 22% of Bankers and Financial Investigators Feel Confident Detecting Crypto-Related Payments
<https://ciphertrace.com/only-22-percent-of-bankers-feel-confident-detecting-crypto-related-payments/>
- 4) October 2020: Crypto Red Flags for Law Enforcement—How to know if your investigation involves cryptocurrency
<https://ciphertrace.com/crypto-red-flags-for-law-enforcement/>
- 5) August 2020: Tracing Ransomware: CipherTrace Helps McAfee Follow NetWalker Funds
<https://ciphertrace.com/tracing-ransomware-ciphertrace-helps-mcafee-follow-netwalker-funds/>
- 6) May 2020: UTXO vs Wallet- To- Wallet Tracing in Bitcoin Investigations (Whitepaper)
<https://ciphertrace.com/whitepaper-utxo-vs-wallet-to-wallet-tracing-in-bitcoin-investigations/>
- 7) February 2020: OCC Hits New York Based Bank With First Ever Enforcement Action for Lack of Crypto AML Compliance
<https://ciphertrace.com/occ-hits-new-york-based-bank-with-first-ever-enforcement-action-for-lack-of-crypto-aml-compliance/>
- 8) February 2020: Fighting Human Trafficking by Following the Money
<https://ciphertrace.com/fighting-human-trafficking-by-following-the-money/>
- 9) December 2019: ALERT: Tracing extorted bitcoin
<https://ciphertrace.com/alert-tracing-extorted-bitcoin/>

Ms. Clegg has also appeared on several broadcast and webinars presenting lectures and teachings on cryptocurrency, including:

1. Cryptocurrency Presentation at the 5th Global Conference on Criminal Finances and Cryptocurrencies on 7 December 2021. The virtual event was co-organized by the Basel Institute on Governance, INTERPOL and Europol.
<https://www.youtube.com/watch?v=q6GKVKwWz0s>
2. Virginia Tech Department of Computer Science. Ms. Clegg discussed the ways that blockchains and cryptocurrencies can facilitate tracing cyber crimes and ransom payouts. She also discussed the ways that CipherTrace operates when tracking financial transactions and examine several case studies from their recent Anti-Money Laundering Report.
https://www.youtube.com/watch?v=_DPEj9OfzHw

3. Cops & Robbers – REIMAGINE v 6.0 #11. Ms. Clegg sits down with Yonah Hochhauser from REIMAGINE 2021 to talk about what makes a good regulator, why crime on the blockchain can be solved, and the new world of non-geographical jurisdictions.
<https://cryptonews.com/videos/cops-robbers-why-crime-on-blockchain-is-easy-to-solve.htm>
4. LinkedIn Live – Data Connectors. Interview with Dawn Morrissey (CEO) and Michael Hiskey (CSO) to discuss financial crimes and ransomware involving cryptocurrency. Discussion emphasizes asset recovery in criminal cases.
https://www.youtube.com/watch?v=0-wSksy_aq4
5. Lightning Talks: Game-Changing Proposals for the Internet.
<https://www.youtube.com/watch?v=gYdYj6A2gWI>
6. True Crime Stories From the World of Crypt Hacks and Ransomware. Ms. Clegg shares a story of how CipherTrace teamed up with McAfee to tackle NetWalker ransomware, a ransomware that has become a franchise within the cybercrime underworld.
<https://www.youtube.com/watch?v=5bHseR7a8zw>
7. Cut Off the Case: Cryptocurrency and Ransomware Payments. Ms. Clegg joins a panel of experts to discuss ransomware and tracking ransomware payments.
<https://www.youtube.com/watch?v=mt8AzHrMX-0>

Part II: Background and Summary of Findings

1. Background on Virtual Currency

In understanding virtual currency investigations, some background on the terminology surrounding virtual currency is useful. Some key terms are discussed below.

Fiat Currency. Government issued currency that have a face value exceeding any commodity value. Fiat is not backed by a commodity like gold. Most paper money issued by governments like the U.S. Dollar (USD) is fiat currency.

Virtual Currency. A digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like digital fiat currency. Popular virtual currencies that are *not* also cryptocurrencies include Robux (for the online platform Roblox) and V-Bucks (for the online game Fortnite).

Cryptocurrency. Cryptocurrency is a type of virtual currency that utilizes cryptography to validate and secure transactions that are digitally recorded on a distributed ledger, such as a blockchain. The first block on the blockchain is referred to as the “genesis block.” This is the beginning of that cryptocurrency. Cryptocurrency allows for decentralized control as opposed to using centralized electronic money and banking systems. The most recognizable and valuable cryptocurrency is bitcoin (BTC), which was launched in 2009 via the Bitcoin blockchain. In 2021, bitcoin peaked at over \$60,000.00 USD to 1 BTC. Ethereum (ETH) is another valuable and popular cryptocurrency, which has reached a value of more than \$4,000.00 to 1 ETH in 2021. Other popular cryptocurrencies include Litecoin (LTC), Cardano (ADA), and Bitcoin Cash (BCH).

Cryptocurrency Exchange. Digital marketplace where one can purchase or trade cryptocurrencies. Some of the top cryptocurrency exchanges include Binance, Coinbase, Gemini, Kraken, and FTX. At those exchanges, customers are allowed to hold, send and receive cryptocurrency to different accounts and addresses. Users can trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies. Exchanges may accept credit card payments, wire transfers or other forms of payment in exchange for digital currencies or cryptocurrencies. A cryptocurrency exchange can be a market maker that typically takes the bid–ask spreads as a transaction commission for its service or, as a matching platform, simply charges fees.

Stablecoin. A type of cryptocurrency pegged to a currency like the U.S. dollar, a commodity such as gold, or algorithmically pegged to other cryptocurrencies. Stablecoins purport to offer the benefits of cryptocurrencies but with the more-stable valuations of certain fiat currencies.

Blockchain Analysis. Cryptocurrency blockchains are available to the public and reviewable on several platforms (*e.g.*, Blockchain.com). Analysis of a blockchain can reveal, among other things, transactional history, trading frequency, block timing, and the total number of blocks.

Fork. A fork occurs when there is a change to the blockchain protocol of a cryptocurrency. A fork is always based on the original blockchain such that all transactions from the original blockchain are copied onto the subsequent blockchain(s).

- Hard Fork. A change to the blockchain protocol which is incompatible with previous versions and therefore creates a new blockchain. Examples of cryptocurrencies that have been created from a hard fork include Bitcoin SV, Bitcoin Cash, and Bitcoin Gold.
- Soft Fork. A change to the blockchain protocol that is compatible with previous versions and therefore does not create a new blockchain.

Mining. The process of solving complex mathematical calculations that confirm cryptocurrency transactions and, as payment, provides the “miner” newly generated units of the underlying cryptocurrency. Mining is essential to maintaining the blockchain ledger and can be conducted by an individual or a mining pool .

Proof of Stake. A way of earning rewards for holding certain cryptocurrencies. A holder of a cryptocurrency gets selected to add the latest batch of transactions to the blockchain and earn some crypto in exchange. The exact details vary by project, but in general proof of stake blockchains employ a network of “validators” who contribute — or “stake” — their own crypto in exchange for a chance of getting to validate new transaction, update the blockchain, and earn a reward.

Proof of Work. The original crypto consensus mechanism, first used by Bitcoin. Proof of Work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system. It is used widely in cryptocurrency mining, for validating transactions and mining new tokens. PoW at scale requires huge amounts of energy, which only increases as more miners join the network.

Wash Trading. Artificially inflating transaction volumes to misrepresent the market for a virtual currency and increase its value. These actions may include traders working with brokers or the deployment of a “bot” making online trades to show increased activity.

2. Background on Regulatory Requirements for Virtual Currencies

Virtual currencies are subject to regulation in the United States by multiple government agencies, including:

- a) SEC and CFTC have certain regulations that apply to virtual currencies. *See, e.g.,* Securities & Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207, July 25, 2017); Commodity Futures Trading Commission, *A CFTC Primer on Virtual Currencies* (Oct. 17, 2017).

- b) U.S. Treasury via FinCEN has registration and reporting requirements for virtual currency exchanges. *See, e.g.,* FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (FIN-2013-G001, Mar. 18, 2013).
- c) IRS requires that taxes be paid on profits from virtual currency. *See, e.g.,* Internal Revenue Service, *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply* (Mar. 25, 2014).

3. Summary of MyBigCoin Investigation Findings

Ms. Clegg investigated My Big Coin (“MBC”) and developed certain findings, including the following summarized findings:

- a) MBC purported to offer a virtual currency and a virtual currency exchange service between (at least) approximately 2014 and 2017. During that period, MBC also made claims about its virtual currency, including that it was a cryptocurrency that could be mined and that the cryptocurrency was backed by gold.
- b) Based on blockchain analysis, MBC was not available as a cryptocurrency until June 28, 2017.
- c) A review of public databases (*e.g.,* Coinlib.io and CoinGecko), cryptocurrency exchanges (*e.g.,* Nova Exchange), and MBC’s statements (*e.g.,* Facebook and Twitter) also suggest that MBC was not traded as a cryptocurrency until after June 28, 2017.
- d) Once MBC was being traded as a cryptocurrency, the trading that occurred is indicative of wash trading, and several other abnormalities were observed with the protocol, transactions, block height, and coin distribution.
- e) CipherTrace analysts observed signs of wash trading through multiple transactions.
- f) Other abnormalities with MBC’s business practices include that MBC did not comply with regulatory and reporting requirements, including those of FinCEN and IRS.

Part III: The Bases and Reasons for the Findings

Various methods and sources were used to conduct this investigation and form opinions. Common methods of investigating virtual currency and cryptocurrency include:

1. Review any reports made to government regulatory agencies (*e.g.*, SEC, CFTC, FinCEN, or IRS).
2. Review statements made by the company, its founders, and its customers or users, including statements made online and through social media.
3. If the virtual currency company claimed to be offering a cryptocurrency, review available blockchain data and look for other evidence to validate any findings, including information from cryptocurrency exchanges and public databases.

Each are addressed below.

1. Regulatory Reporting

A review of MBC's regulatory compliance record revealed the following:

- a) According to the IRS, MBC did not file tax returns. *See* Appendix F.
- b) According to FinCEN, MBC did not register with the U.S. Treasury. *See* Appendix G.
- c) According to the CFTC, Mr. Crater was the owner of MBC and MBC never registered with the CFTC. *See* Appendix H.

2. Statements by Crater, MBC, and MBC's Customers and Users

Various statements demonstrated that MBC was making claims about its virtual currency and related services, including that MBC operated as a cryptocurrency. These statements included, by way of example:

- a) Randall Crater LinkedIn Statements. Examples of statements from Mr. Crater's LinkedIn page (previously available at www.linkedin.com/in/randall-crater-699a8663/, and available in Appendix A) include:
 - i. "We are the only Cryptocurrency to be backed by Gold!"
 - ii. "Send money \$\$\$ in seconds anywhere in the world!"
 - iii. "MyBigCoin Inc is the only Commercial based Cryptocurrency in the World!"
- b) MBC Website Statements. Examples of statements from MBC's website (previously available at www.mybigcoin.com, and samples available in Appendix B) include:
 - i. "Send MBC to anyone, instantly"

- ii. “Mine them”
 - iii. “My Big Coin coming to a merchant near you”
 - iv. “MY BIG COIN is quoted, at the currency value of the coin of that day”
 - v. Picture of the “My Big Coin” Mastercard logo
 - vi. Links to an MBC Exchange, YouTube, Facebook, and Twitter
- c) MBC Exchange Website Statements. The MBC Exchange’s website (previously available at mybigcoinexchange.com, and samples available in Appendix C) reflected:
- i. Offers to sell or buy MBC, and the exchange price.
 - ii. The Exchange did not indicate that it is facilitating the transfer of cryptocurrencies using a blockchain, but instead people trading dollars for an MBC virtual currency.
 - iii. The Exchange did not indicate that Coins can be traded for anything but U.S. dollars.
- d) MBC on YouTube. Examples of statements made in an MBC YouTube video (previously available at <https://youtube.com/watch?v=PSPdcdW7lOQ&t>) include:
- i. “First decentralized virtual currency”
 - ii. “Several currency exchanges exist where you can trade your MyBigCoins for dollars, euros and more.”
- e) MBC on Facebook and Twitter. Examples of images and posts from the MBC’s Facebook and Twitter pages (available in Appendix D and Appendix E) include:
- i. References to MBC offering a cryptocurrency prior to June 28, 2017.
 - ii. References to MBC offering a cryptocurrency after June 28, 2017, including references to cryptocurrency exchanges and databases.

3. Blockchain Analysis and Related Investigatory Steps

a) When MBC Cryptocurrency Trading Began

MBC claimed to offer a cryptocurrency, leading the investigation to conduct blockchain analysis of the MBC blockchain and look for other evidence to validate any findings. Blockchain analysis revealed that MBC was first available as a cryptocurrency on June 28, 2017, the date of the genesis block the the MBC blockchain. There is no evidence of a “fork” on the MBC blockchain prior to that date. These findings are congruent with certain public statements made by MBC. For example, while MBC had previously made references to its cryptocurrency, the public ledger was only published after June 28, 2017.

The investigation also searched multiple exchanges for “My Big Coin” and “MBC” and reviewed public databases that track virtual currencies trading history and value (e.g., Coin Gecko and CoinLib). These investigatory steps did not reveal evidence that MBC was trading as a cryptocurrency prior to June 28, 2017. There was evidence of MBC being traded as a

cryptocurrency on Nova Exchange (novaexchange.com). Nova Exchange was an altcoin cryptocurrency exchange based in Sweden. The exchange closed in October of 2019 and there were a multitude of screen captures available on the web.archive.org. According to information available on the web.archive.org, MBC was trading on Nova Exchange on September 3, 2017. This was the earliest that the link novaexchange.com/markets was captured by web.archive.org.¹

b) Analysis of MBC Cryptocurrency Trading

After June 28, 2017, the trading of MBC was indicative of “wash trading” and there were also several abnormalities with the protocol, transactions, block height, and coin distribution, including:

- Lack of white or yellow papers describing the work and offering insight into the project. While not mandatory, it is typical practice within the technology realm to publish the details of a particular technology. A yellow paper is a theoretical explanation of the product. White papers are commonly used to describe the theory behind a new technology of computer methodology.
- The lack of evidence of a variety of users.
- The lack of transparency into the protocol’s transaction validation system, MBC never clearly defined whether its blockchain was Proof of Work or Proof of Stake and the manner in which the blockchain disbursed newly created MBC. The MBC blockchain appeared to function as proof of work.
- A lack of open-source software related to the distributed ledger.
- The link provided by GitHub for the MBC public code was for a wallet, not a blockchain or any type of ledger code.
- Analysis of individual blocks showed the majority of blocks had a single transaction contained in them. By contrast, Bitcoin blocks typically have several thousands of transactions in each block. Single-transaction blocks could cause several issues, the most notable of which is the inability to scale and lack of efficiency.
- A high number of blocks in a short period that is not congruent with other blockchain activity with similar block times and structure.²

¹ MBC Twitter provided a link to the Nova Exchange on July 28, 2017. On June 21, 2018, MBC Twitter also provided a link to CryptoBridge, but there are no screen captures from web.archive.org to validate whether MBC was ever listed on that exchange. GitHub also purported to provide a link to MBC’s public code. GitHub’s website also does not reflect MBC cryptocurrency trades prior to June 2017.

² The MBC blockchain started on June 28, 2017 and reached block height 686889 on September 18, 2020.

- MBC blockchain demonstrated erratic block times. Most blockchains have a discernable average block time (*e.g.*, Bitcoin which averages 10 minutes, Ethereum averages 13-15 seconds, and Dash about 2 minutes 30 seconds). The average number of blocks during the first phase of MBC was 1263.73 blocks per day, whereas during the second phase it decrease significantly to 343.55 blocks per day.
- A sample of the MBC block times shows not only erratic times, but also mistimed blocks.
- As indicated in the original report, CipherTrace analysts observed signs of wash trading when MBC demonstrated many transactions from same address to same address. In a similar fashion to money laundering, transaction from one account to one account often are superfluous or done for obfuscation.
- Most users conducting crypto transactions compare this to a price point like the U.S. Dollar or a predetermined amount of crypto for payment of services or goods. Therefore, transactions of exact and round numbers in BTC are not the majority. For instance, as of 04/13/2022 @ 4:38pm eastern time, \$1500.00 is equal to 0.036 BTC. While .050 BTC is equal to \$2058.95 USD. MBC transactions routinely registered as exact, round numbers.